

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-328033

(43)Date of publication of application : 30.11.1999

(51)Int.Cl. G06F 12/14
G06F 17/60
G09C 1/00

(21)Application number : 10-138663

(71)Applicant : FUJITSU LTD

(22)Date of filing : 20.05.1998

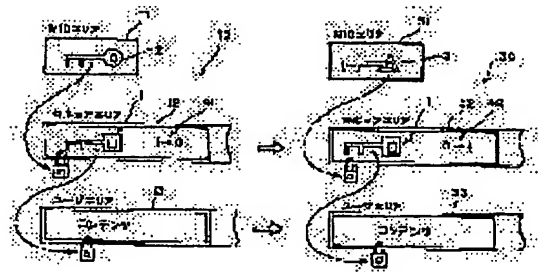
(72)Inventor : UCHIUMI KENICHI
HIRANO HIDEYUKI
KOTANI MASATAKE

(54) LICENSE TRANSFER DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To copy and deliver contents while protecting a person having a right to the use of the contents in a license transfer system which transfers the right to the use of contents.

SOLUTION: Contents are enciphered with a key 1, and this key 1 and information on use right 41 are enciphered with a key 2 consisting of a medium ID which specifies a storage medium 10 where they are stored. At the time of transferring the right to the use of the contents, contents enciphered by the key 1 are transferred to a storage medium 30 of a transfer destination as they are, and the key 1 and use right information 41 are deciphered by the medium ID of the storage medium of the transfer source and are enciphered by the medium ID of the storage medium of the transfer destination and are stored in the storage medium 30 of the transfer destination.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-328033

(43) 公開日 平成11年(1999)11月30日

(51) Int.Cl.⁶

識別記号

F I

G 0 6 F 12/14

3 2 0

G 0 6 F 12/14

3 2 0 A

17/60

G 0 9 C 1/00

6 6 0 D

G 0 9 C 1/00

6 6 0

G 0 6 F 15/21

Z

審査請求 未請求 請求項の数 7 O L (全 13 頁)

(21) 出願番号

特願平10-138663

(22) 出願日

平成10年(1998) 5 月20日

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中 4 丁目 1 番
1 号

(72) 発明者 内海 研一

神奈川県川崎市中原区上小田中 4 丁目 1 番
1 号 富士通株式会社内

(72) 発明者 平野 秀幸

神奈川県川崎市中原区上小田中 4 丁目 1 番
1 号 富士通株式会社内

(72) 発明者 小谷 誠剛

神奈川県川崎市中原区上小田中 4 丁目 1 番
1 号 富士通株式会社内

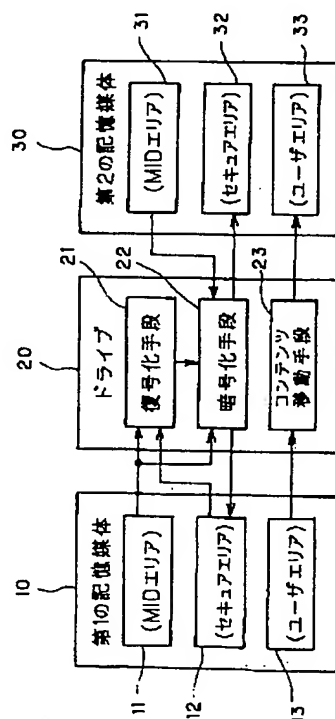
(74) 代理人 弁理士 山田 正紀

(54) 【発明の名称】 ライセンス委譲装置

(57) 【要約】

【課題】本発明は、コンテンツの使用権を委譲するライセンス委譲システムに関し、そのコンテンツに関し権利を有する者の保護を図りつつ、そのコンテンツの複製や頒布等を行なう。

【解決手段】鍵1でコンテンツを暗号化し、その鍵1および使用権情報41を、それらが格納された記憶媒体10を特定するメディアIDからなる鍵2で暗号化しておき、そのコンテンツの使用権を委譲するにあたり、コンテンツは鍵1で暗号化された状態のまま、委譲先の記憶媒体30に移し、鍵1および使用権情報41を移転前の記憶媒体10のメディアIDで復号化し、さらに委譲先の記憶媒体30のメディアIDで暗号化して、委譲先の記憶媒体30に格納する。



【特許請求の範囲】

【請求項 1】 所定の鍵により暗号化されたコンテンツと、自分を特定する第 1 のメディア ID と、前記鍵と該コンテンツの使用権を表す第 1 の使用権情報との双方が一緒あるいは別々に前記第 1 のメディア ID で暗号化されてなる第 1 の暗号化セキュア情報とが格納された第 1 の記憶媒体と、自分を特定する第 2 のメディア ID が格納された第 2 の記憶媒体とをアクセスして前記第 1 の記憶媒体に格納されたコンテンツの使用権を前記第 1 の記憶媒体から前記第 2 の記憶媒体に委譲するライセンス委譲装置において、

前記コンテンツの使用権の委譲にあたり前記第 1 の記憶媒体に格納された第 1 の暗号化セキュア情報を前記第 1 のメディア ID を用いて復号化することにより前記鍵と前記第 1 の使用権情報とを得る復号化手段、および前記復号化手段による復号化により得られた鍵と、前記復号化手段による復号化により得られた第 1 の使用権情報があらず第 1 の使用権が譲渡あるいは分与された第 2 の使用権をあらず第 2 の使用権情報との双方を一緒にあるいは別々に前記第 2 のメディア ID で暗号化することにより第 2 の暗号化セキュア情報を生成して前記第 2 の記憶媒体に格納させる暗号化手段を備えたことを特徴とするライセンス委譲装置。

【請求項 2】 前記暗号化手段が、さらに、前記第 1 の使用権から前記第 2 の使用権を差し引いた後の第 3 の使用権をあらず第 3 の使用権情報を、あるいは前記鍵と該第 3 の使用権情報との双方を、前記第 1 のメディア ID で暗号化して前記第 1 の記憶媒体に書き戻すことにより、該第 1 の記憶媒体に、前記第 1 の暗号化セキュア情報に代えて、前記鍵と前記第 3 の使用権情報との双方が該第 1 のメディア ID で暗号化されてなる第 3 の暗号化メディア情報を格納させるものであることを特徴とする請求項 1 記載のライセンス委譲装置。

【請求項 3】 前記第 1 の記憶媒体が持つ前記コンテンツの使用権全体を前記第 2 の記憶媒体に委譲する場合に、前記暗号化手段が、前記復号化手段による復号化により得られた鍵と、前記第 1 の使用権の全てを受け継いだ第 2 の使用権をあらず第 2 の使用権情報とが暗号化されてなる第 2 の暗号化セキュア情報を生成して前記第 2 の記憶媒体に格納させるとともに、前記第 1 の記憶媒体に格納されている前記第 1 の暗号化セキュア情報を構成する前記鍵を破壊させるものであることを特徴とする請求項 1 記載のライセンス委譲装置。

【請求項 4】 コンテンツの使用権委譲前において、前記第 1 の記憶媒体が、暗号化された、使用権を委譲しようとするコンテンツが格納されたものであって、コンテンツの使用権の委譲にあたり、前記第 1 の記憶媒体に格納された、委譲対象の暗号化されたコンテンツを読み出して、暗号化された状態のまま、前記第 2 の記憶媒体に格納するコンテンツ移動手段を備えたことを特徴

とする請求項 1 記載のライセンス委譲装置。

【請求項 5】 前記第 1 の使用権情報および前記第 2 の使用権情報が使用権が存在することをあらわすものであり、前記第 3 の使用権情報が使用権が存在しないことをあらわすものであることを特徴とする請求項 1 記載のライセンス委譲装置。

【請求項 6】 前記第 1 の使用権情報が、第 1 の使用可能回数あるいは使用可能時間をあらわすものであり、前記第 2 の使用権情報が、該第 1 の使用可能回数あるいは使用可能時間以内の第 2 の使用可能回数あるいは使用可能時間をあらわすものであり、前記第 3 の使用権情報が、該第 1 の使用可能回数あるいは使用可能時間から該第 2 の使用可能回数あるいは使用可能時間を差し引いた後の第 3 の使用可能回数あるいは使用可能時間をあらわすものであることを特徴とする請求項 1 記載のライセンス委譲装置。

【請求項 7】 前記第 1 の記憶媒体および前記第 2 の記憶媒体をそれぞれ駆動する第 1 のドライブおよび第 2 のドライブを備えるとともに、該第 1 のドライブおよび該第 2 のドライブが、前記第 1 の記憶媒体および前記第 2 の記憶媒体それぞれをアクセスする、それぞれ第 1 のファームウェアおよび第 2 のファームウェアを備えたものであり、前記復号化手段および前記暗号化手段が、前記第 1 のファームウェアと前記第 2 のファームウェアとの複合体としてのファームウェア内に構成されたものであって、前記第 1 のファームウェアのみが前記第 1 のドライブにより駆動される前記第 1 の記憶媒体をアクセスする権原を有するとともに、前記第 2 のファームウェアのみが前記第 2 のドライブにより駆動される第 2 の記憶媒体をアクセスする権原を有するものであることを特徴とする請求項 1 記載のライセンス委譲装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コンテンツの使用権を第 1 の記憶媒体から第 2 の記憶媒体に委譲するライセンス委譲装置に関する。

【0002】

【従来の技術】近年、如何にして著作権の保護の実効を図るかが問題となってきた。例えば本のような有形物の場合、頒布すること自体は複製を伴わず、本を転売すればその本は購入者の手もとに渡り販売者のもとには本は存在しなくなり、したがって著作権の保護は比較的簡単であるが、デジタル情報化された著作物の場合、例えばそのデジタル化された著作物をネットワークを介して送信すると自分側と相手側との双方に同じ著作物が発生し、頒布すること自体が複製を伴う結果となり、通常、このようなデジタル情報化された著作物に対する著作権の実効的な保護は極めて難しいとされている。

【0003】

【発明が解決しようとする課題】本発明は、上記事情に鑑み、デジタル化された文書、映画、プログラム等のコンテンツの使用権を、そのコンテンツに関し権利を有する者の保護を図りつつ委譲することのできるライセンス委譲装置を提供することを目的とする。

【0004】

【課題を解決するための手段】上記目的を達成する本発明のライセンス委譲装置は、所定の鍵により暗号化されたコンテンツと、自分を特定する第1のメディアIDと、上記鍵とそのコンテンツの使用権を表す第1の使用情報との双方が一緒あるいは別々に第1のメディアIDで暗号化されてなる第1の暗号化セキュア情報とが格納された第1の記憶媒体と、自分を特定する第2のメディアIDが格納された第2の記憶媒体とをアクセスして第1の記憶媒体に格納されたコンテンツの使用権を第1の記憶媒体から第2の記憶媒体に委譲するライセンス委譲装置において、コンテンツの使用権の委譲にあたり第1の記憶媒体に格納された第1の暗号化セキュア情報を第1のメディアIDを用いて復号化することにより上記鍵と上記第1の使用権情報とを得る復号化手段、および上記復号化手段による復号化により得られた鍵と、および上記復号化手段による復号化により得られた第1の使用権情報があらず第1の使用権が譲渡あるいは分与された第2の使用権をあらわす第2の使用権情報との双方を一緒あるいは別々に上記第2のメディアIDで暗号化することにより第2の暗号化セキュア情報を生成して第2の記憶媒体に格納させる暗号化手段を備えたことを特徴とする。

【0005】ここで、上記本発明のライセンス委譲装置において、上記暗号化手段は、さらに、上記第1の使用権から上記第2の使用権を差し引いた後の第3の使用権をあらわす第3の使用権情報を、あるいは鍵と上記第3の使用権情報との双方を、上記第1のメディアIDで暗号化して第1の記憶媒体に書き戻すことにより、第1の記憶媒体に、上記第1の暗号化セキュア情報に代えて、上記鍵と上記第3の使用権情報との双方が第1のメディアIDで暗号化されてなる第3の暗号化メディア情報を格納させるものであってもよく、あるいは、第1の記憶媒体が持つ上記コンテンツの使用権全体を第2の記憶媒体に委譲する場合に、上記暗号化手段は、上記復号化手段による復号化により得られた鍵と、上記第1の使用権の全てを受け継いだ第2の使用権をあらわす第2の使用権情報とが暗号化されてなる第2の暗号化セキュア情報を生成して第2の記憶媒体に格納させるとともに、第1の記憶媒体に格納されている第1の暗号化セキュア情報を構成する鍵を破壊させるものであってもよい。

【0006】尚、上記の、「鍵と、……第1の使用権情報との双方が一緒あるいは別々に第1のメディアIDで暗号化されてなる第1の暗号化セキュア情報」は、鍵

を第1のメディアIDで暗号化し、これとは別に第1の使用権情報を第1のメディア情報で暗号化し、それらの暗号化された鍵と暗号化された第1の使用権情報とを合わせたものを第1の暗号化セキュア情報と称してもよく、あるいは、鍵と第1の使用権情報との双方を連ねたものを第1のメディア情報で暗号化し、その暗号化された情報を第1の暗号化セキュア情報と称してもよいことを意味している。

【0007】また、上記の、「鍵と、……第2の使用権情報の双方を一緒あるいは別々に……第2のメディアIDで暗号化することにより第2の暗号化セキュア情報を生成して……」や「鍵と、……第3の使用権情報との双方が第1のメディアIDで暗号化されてなる第3の暗号化セキュア情報」も同様である。さらに、上記の、「第3の使用権情報を、あるいは……鍵と……第3の使用権情報との双方を、……第1のメディアIDで暗号化して……」は、鍵と、第1の使用権情報あるいは第2の使用権情報を別々に暗号化するシステムにおいては、第3の使用権情報のみを暗号化すればよく、鍵と第1（あるいは第2）の使用権情報を連ねたものを暗号化するシステムにおいては、鍵と第3の使用権情報との双方を連ねたものを暗号化することを意味している。

【0008】本発明のライセンス委譲装置は、例えばMO（光磁気ディスク）やハードディスクには、それぞれに固有のID（メディアIDと称する）が付されている点に着目し、完成されたものである。所定の鍵で暗号化されたコンテンツを流通させることによりその暗号化されたコンテンツ自体はその鍵を用いて復号化しない限り使用不可能である。そこで、その暗号化されたコンテンツを復号化するための鍵と、使用権情報（例えばそのコンテンツの使用が許可されているか否かという情報など）との双方を、その記憶媒体独自のメディアIDで暗号化しておく。こうすることにより、その暗号化されたコンテンツは、そのコンテンツがもともと格納された記憶媒体を離れてそれ自体が頒布されても使用不能であり、鍵もそのまま頒布したのでは頒布を受けた先ではメディアIDが異なるため鍵を復号化することはできず、したがって使用権のない者による無断使用が防止できる。

【0009】このようなシステムにおいて、自分（第1の記憶媒体）の使用権を委譲先（第2の記憶媒体）に譲り渡すには、自分（第1の記憶媒体）のメディアIDで鍵および自分の使用権情報を復号化し、自分の使用権の範囲（例えば使用可能な残存回数）の中で使用権を分与し（あるいはその使用権全体であってもよい）、鍵と、その分与されたあるいは全体としての使用権情報を、委譲先（第2の記憶媒体）のメディアID（第2のメディアID）で暗号化してその委譲先（第2の記憶媒体）に格納させる。自分（第1の記憶媒体）には、残りの使用権（使用権が存在しないという使用権を含む）を自分

(第 1 の記憶媒体) のメディア ID (第 1 のメディア ID) で暗号化して自分 (第 1 の記憶媒体) に書き戻す。あるいは使用権の全部を委譲する場合は、自分 (第 1 の記憶媒体) では、残りの使用権 (この場合は使用権が存在しないという使用権) を暗号化して書き戻す代わりに、自分 (第 1 の記憶媒体) に暗号化された形式で格納されている鍵を破壊してしまってもよい。こうすることにより、そのコンテンツに関し権利を有する者の権利を犯すことなく使用権の譲渡が可能となる。

【0010】ここで、上記本発明のライセンス委譲装置は、コンテンツの使用権委譲前において、第 1 の記憶媒体が、暗号化された、使用権を委譲しようとするコンテンツが格納されたものであって、コンテンツの使用権の委譲にあたり、第 1 の記憶媒体に格納された、委譲対象の暗号化されたコンテンツを読み出して、暗号化された状態のまま、第 2 の記憶媒体に格納するコンテンツ移動手段を備えることが好ましい。

【0011】コンテンツ自体は暗号化された状態のまま頒布されるので、いつ頒布してもよく、例えば既に頒布されているときは鍵と使用権のみを渡せばよいが、例えば上記のコンテンツ移動手段を備えて、コンテンツの使用権の委譲にあたりそのコンテンツを第 1 の記憶媒体から第 2 の記憶媒体に移動 (複製) してもよい。また、上記本発明のライセンス委譲装置において、上記第 1 の使用権情報および上記第 2 の使用権情報が使用権が存在することをあらわすものであり、上記第 3 の使用権情報が使用権が存在しないことをあらわすものであってもよく、あるいは、上記第 1 の使用権情報が、第 1 の使用可能回数あるいは使用可能時間をあらわすものであり、上記第 2 の使用権情報が、その第 1 の使用可能回数あるいは使用可能時間以内の第 2 の使用可能回数あるいは使用可能時間をあらわすものであり、上記第 3 の使用権情報が、第 1 の使用可能回数あるいは使用可能時間から第 2 の使用可能回数あるいは使用可能時間を差し引いた後の第 3 の使用可能回数あるいは使用可能時間をあらわすものであってもよい。

【0012】このほか、例えば使用権を有する人を特定する ID を使用権情報としてもよく、使用権情報は、使用権の有無や範囲をあらわす情報であればどのような情報であってもよい。また、上記本発明のライセンス委譲装置において、第 1 の記憶媒体および第 2 の記憶媒体をそれぞれ駆動する第 1 のドライブおよび第 2 のドライブを備えるとともに、第 1 のドライブおよび第 2 のドライブが、第 1 の記憶媒体および第 2 の記憶媒体それぞれをアクセスする、それぞれ第 1 のファームウェアおよび第 2 のファームウェアを備えたものであり、上記復号化手段および上記暗号化手段が、上記第 1 のファームウェアと上記第 2 のファームウェアとの複合体としてのファームウェア内に構成されたものであって、上記第 1 のファームウェアのみが第 1 のドライブにより駆動される第 1

の記憶媒体をアクセスする権原を有するとともに、上記第 2 のファームウェアのみが第 2 のドライブにより駆動される第 2 の記憶媒体をアクセスする権原を有するものであることが好ましい。

【0013】ここで、「第 1 のファームウェアのみが…第 1 の記憶媒体をアクセスする権原を有する」、「第 2 のファームウェアのみが…第 2 の記憶媒体をアクセスする権原を有する」は、例えばアプリケーションプログラム等からは、それら第 1 のファームウェアや第 2 のファームウェアを介在させずに直接には第 1 の記憶媒体や第 2 の記憶媒体をアクセスすることはできないように構成されていることを意味し、このような構成を備える以下のような場合を含め、コンテンツに関する正当な権利を有する者の権利が一層確実に保護されることになる。

【0014】すなわち、仮に、ファームウェアを介在させずにアプリケーションプログラムから直接に記憶媒体をアクセスすることができるシステムの場合、第 1 の記憶媒体から第 2 の記憶媒体に使用権を委譲する前にアプリケーションプログラムで第 1 の記憶媒体を直接にアクセスして上述した第 1 の暗号化セキュア情報を読み出して第 3 の記憶媒体に格納しておく。このような前準備を行なった上で使用権を第 1 の記憶媒体から第 2 の記憶媒体に委譲する。その委譲が終了した後、再びアプリケーションプログラムで第 1 の記憶媒体を直接にアクセスして第 3 の記憶媒体にあらかじめ複製しておいた委譲前の第 1 の暗号化セキュア情報を第 1 の記憶媒体に書き戻す。この場合、第 1 の記憶媒体は使用権を委譲する前の状態に戻り、かつ第 2 の記憶媒体にも使用権が発生し、正当な権利者の権利が犯される結果をもたらす。

【0015】そこで、上記のようにファームウェアのみからアクセスを可能とすることにより、上記のような不正の発生を未然に防止することができ、正当な権利者の権利をより一層確実に保護することができる。

【0016】

【発明の実施の形態】以下、本発明の実施形態について説明する。ここでは解り易さのため、概念的な実施形態について先ず説明し、次いで具体的な実施形態について説明する。図 1 は、本発明のライセンス委譲装置の一実施形態を示す構成図、図 2 は、その説明のための模式図である。

【0017】図 1 には、第 1 の記憶媒体 10、ドライブ 20、および第 2 の記憶媒体 30 が示されている。第 1 の記憶媒体 10 および第 2 の記憶媒体 30 は、いずれも、その記憶媒体の種類を問うものではないが、その記憶媒体を特定するメディア ID を有することが必要である。このメディア ID は、同種の記憶媒体を互いに確実に識別するものである必要はなく、例えば同一のメディア ID を持つ 2 つの記憶媒体が出会うことがほとんど期待できない程度にその記憶媒体にユニークなものであれ

ばよい。

【0018】ドライブ20は、本実施形態では、第1の記憶媒体10を駆動する第1のドライブ、例えば第1の記憶媒体10がMO（光磁気ディスク）の場合の光磁気ディスクドライブ装置と、第2の記憶媒体30を駆動する第2のドライブ、例えば第2の記憶媒体30がハードディスクの場合そのハードディスクを駆動するハードディスクドライブ装置との複合体として観念される。

【0019】また、第1のドライブには、そのマイクロコンピュータとそのマイクロコンピュータで動作するソフトウェアとの組合せからなる、第1のドライブにより駆動される第1の記憶媒体をアクセスするための第1のファームウェアが搭載されており、これと同様に、第2のドライブにも、マイクロコンピュータとそのマイクロコンピュータで動作するソフトウェアとの組合せからなる、その第2のドライブにより駆動される第1の記憶媒体をアクセスするための第2のファームウェアが搭載されている。ここでは、第1のファームウェアと第2のファームウェアとの複合体としてのファームウェアがドライブ20に搭載されているものと観念する。

【0020】第1の記憶媒体10および第2の記憶媒体20は、それぞれ、自分自身のメディアIDを記憶しておくMIDエリア11、31、使用権情報やその他コンテンツの属性に関する情報が格納されるセキュアエリア12、32、およびコンテンツ自身が格納されるユーザエリア13、33を有する。ここでは、第1の記憶媒体10が持っているコンテンツの使用権を第2の記憶媒体30に委譲しようとしており、したがってここでは、第1の記憶媒体10のMIDエリア11、セキュアエリア12、およびユーザエリア13には、それぞれ、その第1の記憶媒体10のメディアID、使用権情報やその他の属性、およびコンテンツが実際に格納されているものとする。

【0021】一方、第2の記憶媒体30のMIDエリア31には、その第2の記憶媒体30のメディア30のメディアIDが格納されているが、セキュアエリア32、およびユーザエリア33はあらかじめ領域として用意されていてもよく、あるいは、コンテンツの使用権の委譲にあたってそれらの領域が生成されるものであってもよい。

【0022】以下において説明する復号化手段21、暗号化手段22、およびコンテンツ移動手段23は、ドライブ20内に搭載されたファームウェア内に構築されており、アプリケーションプログラムは、そのファームウェアを起動することはできるが、そのファームウェアの動作の内部に入り込んでそのファームウェアの動作を制御したり、あるいはそのファームウェアを介在させずに第1の記憶媒体や第2の記憶媒体を直接にアクセスすることはできないように構成されている。

【0023】つまり、MIDエリア11、31は、ファ

ームウェアによるリードが許可されライトが禁止されているエリアであり、アプリケーションは、ファームウェアを介在させた場合を含めて原則としてMIDエリア11、31へのアクセスが禁止されている。また、セキュアエリア12、32とユーザエリア13、33はファームウェアによるリード・ライトが許可されているエリアであり、アプリケーションは、本実施形態では、ファームウェアを介在させた場合にのみセキュアエリア12、32とユーザエリア13、33にアクセスすることができ、直接リード・ライトを行うことはできない。但し、ユーザエリア13、33については、アプリケーションによる直接的なアクセスが許可されたエリアであってもよい。

【0024】尚、MIDエリア11、31については、セキュアエリア12、32およびユーザエリア13、33とは独立に物理的に書き換え不可能な不揮発性の記憶媒体上に設けられていることが望ましい。但し、本実施形態ではMIDエリアはセキュアエリアおよびユーザエリアとともに第1の記憶媒体および第2の記憶媒体上に設けられている。

【0025】ここで、図2に示すように、第1の記憶媒体10のユーザエリア13に格納されたコンテンツは、鍵1で暗号化された形式で格納されており、その鍵1は、使用権情報41とともに、MIDエリア11に格納された、この第1の記憶媒体10のメディアIDからなる鍵2で暗号化された形式で、セキュアエリア12に格納されている。ここで、図2には、セキュアエリア12に格納された使用権情報41として、‘1→0’が示されているが、‘1’はそのコンテンツの使用権が存在することを意味し、‘0’はそのコンテンツの使用権が無いことを意味し、‘1→0’は、使用権の委譲前は‘1’であって、使用権委譲の際に‘0’に書き換えられることを意味している。また、図2において、セキュアエリア12およびユーザエリア13は、右にさらに延びるように描かれているが、これは、1つの記憶媒体（ここでは第1の記憶媒体10）のユーザエリアに複数のコンテンツが格納され、それら複数のコンテンツそれぞれについて鍵や使用権情報等がセキュアエリア12に格納される場合があることを意味している。

【0026】ここで鍵1と使用権情報41を鍵2で暗号化するにあたっては、この図2では、鍵1と使用権情報41とを合わせた情報が鍵2で暗号化されているように描かれてはいるが、そうであってもよく、あるいは、鍵1が鍵2で暗号化され、それとは別に、使用権情報41が鍵2で暗号化されているように描かれていてもよい。いずれの場合であっても、鍵2で暗号化された鍵1と、鍵2で暗号化された使用権情報との双方を合わせたものを、ここでは暗号化セキュア情報（本発明にいう第1の暗号化セキュア情報）と称する。

【0027】コンテンツの使用権の委譲にあたり、図1

に示すドライブ 20 の復号化手段 21 により、第 1 の記憶媒体 10 の MID エリア 11 に記憶された、第 1 の記憶媒体 10 のメディア ID (本発明にいう第 1 のメディア ID) からなる鍵 2 で、セキュアエリア 12 に格納された第 1 の暗号化セキュア情報が復号化され、その暗号化により平文の鍵 1 と使用権情報 41 (ここでは、使用権が存在することを表わす '1') が取り出される。そこで、今度は、図 1 に示すドライブ 20 の暗号化手段 22 により、その復号化により平文に戻された鍵 1 と使用権情報 41 (使用権が存在することをあらわす '1') が今度は、第 2 の記憶媒体 30 の MID エリア 31 に格納されたメディア ID (本発明にいう第 2 のメディア ID) からなる鍵 3 で暗号化されて第 3 の暗号化セキュア情報が生成され、第 2 の記憶媒体 30 のセキュアエリア 32 に格納される。図 2 における第 2 の記憶媒体 30 のセキュアエリア 32 に描かれた使用権情報 42 が '0 → 1' となっているのは、使用権の委譲を受ける前は使用権が存在せず '0' であって、使用権の委譲を受けることにより使用権が存在することをあらわす '1' に書き換えられたことを意味する。

【0028】また、第 1 の記憶媒体 10 には、復号化された使用権情報 41 が、使用権が存在しないことをあらわす '0' に書き換えられ、復号化された鍵 1 と、使用権が存在しないことをあらわす使用権情報が、第 1 の記憶媒体 10 のメディア ID からなる鍵 2 で暗号化されて、新たな暗号化セキュア情報 (本発明にいう第 3 のセキュア情報) が生成され、それまで第 1 の記憶媒体 10 のセキュアエリア 12 に格納されていた第 1 の暗号化セキュア情報に代えて、その新たに生成された第 3 のセキュア情報がそのセキュアエリア 12 に格納される。

【0029】あるいは、第 1 の記憶媒体 10 にはそのコンテンツの使用権が存在しなくなったのであるから鍵 1 は不要であり、第 3 のセキュア情報を生成して第 1 の記憶媒体 10 のセキュアエリア 12 に格納することに代え、そのセキュアエリア 12 に暗号化された形式で格納されている鍵 1 を破壊してしまってもよい。また、第 1 の記憶媒体 10 のユーザエリア 13 に格納されている、鍵 1 で暗号化されたコンテンツは、図 1 に示すドライブ 20 のコンテンツ移動手段 23 により、第 1 の記憶媒体 10 から読み出され、鍵 1 により暗号化された状態のまま、第 2 の記憶媒体 30 のユーザエリア 33 に格納される。

【0030】以上により、それまで第 1 の記憶媒体 10 が所有していた、コンテンツの使用権が、第 2 の記憶媒体 20 に委譲される。それ以降、第 2 の記憶媒体 20 を駆動する第 2 のドライブでは、アプリケーションプログラムからの、このコンテンツの読み出し要求があると、その第 2 のドライブに搭載された第 2 のファームウェアは、第 2 の記憶媒体 30 をアクセスし、その第 2 の記憶媒体 30 の MID エリア 31 に格納された、その第 2 の

記憶媒体 30 のメディア ID からなる鍵 3 で、セキュアエリア 32 に格納された暗号化セキュア情報を復号化し、使用権が存在することを確認し、鍵 1 により、ユーザエリア 33 に格納された、暗号化されたコンテンツを復号化し、その復号化されたコンテンツをアプリケーションプログラムに戻す。

【0031】一方、その使用権を委譲した後は、第 1 の記憶媒体 10 を駆動する第 1 のドライブでは、仮に、アプリケーションプログラムからの、その使用権を委譲したコンテンツの読み出し要求があった場合、その第 1 のドライブに搭載された第 1 のファームウェアは、第 1 の記憶媒体 10 をアクセスし、その第 1 の記憶媒体の MID エリアに格納された、その第 1 の記憶媒体 30 のメディア ID からなる鍵 2 で、そのセキュアエリア 12 に格納された暗号化セキュア情報を復号化し、使用権の存在を確認したところ使用権が存在しないことを認識し、あるいは、上述の、鍵 1 を破壊するシステムの場合は、鍵 1 が破壊されていること、あるいはそのコンテンツを復号化できないことを認識し、アプリケーションプログラムに対し、そのコンテンツは読み出し不能である旨通知する。このようにして、コンテンツの使用権を、そのコンテンツに関し権利を有する者の権利を犯すことなく、有効に委譲することができる。

【0032】ここで、上記実施形態では、簡単のため、使用権情報は、使用権が存在することをあらわす '1' と使用権が存在しないことをあらわす '0' との二値情報であるとして説明したが、使用可能回数を使用権情報として用いてもよい。例えば委譲前の第 1 の記憶媒体 10 の使用権情報が使用可能回数 10 回をあらわす '100' であったものとし、その使用可能回数の一部、例えば使用可能回数 3 回分のみを第 2 の記憶媒体 30 に委譲してもよい。この場合、第 2 の記憶媒体 30 の使用権情報は使用可能回数 3 回をあらわす '3' となり、第 1 の記憶媒体 10 には、使用権情報として、使用可能回数 7 回をあらわす '7' が書き戻される。第 1 の記憶媒体 10 あるいは第 2 の記憶媒体 30 でそのコンテンツが使用されると、その使用のたびに、第 1 のドライブに搭載された第 1 のファームウェアあるいは第 2 のドライブに搭載された第 1 のファームウェアにより、その第 1 の記憶媒体 10 あるいは第 2 の記憶媒体 30 の使用可能回数が 1 ずつ減算される。

【0033】ここで、第 2 の記憶媒体 30 に委譲した 3 回分の使用権を使い切ってしまったとき、第 1 の記憶媒体 10 に未だ使用権が残っていればその使用権の一部もしくは全部を上記と同一の手順で再度第 2 の記憶媒体に委譲することもできる。ただしその場合は、暗号化されたコンテンツ自体は既に第 2 の記憶媒体 30 に移っているため、そのコンテンツ自体を第 2 の記憶媒体 30 に移す必要はなく、そのコンテンツの使用権のみを第 2 の記憶媒体 30 に移せばよい。

【0034】尚、図2に示す例では、鍵1と使用権情報との双方を1つの情報と見なして、その情報を鍵2で暗号化することにより第1の記憶媒体10用の暗号化セキュア情報を生成し、鍵1と使用権情報との双方を1つの情報とみなしてその情報を鍵3で暗号化することにより第2の記憶媒体30用の暗号化セキュア情報を生成しているが、鍵1と使用権情報は、別々に暗号化してもよい。その場合、使用権の委譲にあたって鍵1は既に暗号化された形式で第1の記憶媒体10に格納されているため、新たな使用権情報のみを暗号化して第1の記憶媒体10に書き戻せばよい。また、使用可能回数を複数回に分けて委譲する場合、2回目以降の委譲の際は、第2の記憶媒体30には鍵1が鍵3で暗号化された形式で既に格納されているため、委譲を受けた使用可能回数をあ

らわす使用権情報のみを鍵3で暗号化してセキュアエリア32に書き込めばよい。

【0035】また、鍵1と使用権情報のほか、例えばそのコンテンツの名称、そのコンテンツの最終アクセス日時等そのコンテンツの使用権情報以外の属性も一緒にセキュアエリアに格納してもよく、その場合に、それらの属性が暗号化する必要がないものである場合は平文のまま格納してもよく、あるいはそれらの属性が暗号化する必要がないものであっても、鍵1や使用権情報と一緒に暗号化してもよい。

【0036】さらに、上記では使用権情報として、使用権の有無と、使用回数を取り挙げて説明したが、そのほかにも、使用可能時間を使用権情報としてもよく、アクセスが許諾された人をあらかずIDを使用権情報としてもよく、使用権の有無、あるいは使用可能範囲をあらかず種々の情報を使用権情報として使用することができる。

【0037】図3は、本発明のライセンス委譲装置の一実施形態が搭載されたコンピュータシステムの一例を示す外観斜視図、図4は、そのコンピュータシステムの構成を示すブロック図である。このコンピュータシステム50は、外観上は、図3に示すように、CPUやメモリ等が内蔵された本体部51、表示画面52a上に画像を表示する画像表示装置52、このコンピュータシステム50に対し各種の指示を行なうための操作子であるキーボード53、および画像表示装置52の表示画面52a上の位置を指定するための操作子であるマウス54により構成されている。また本体部51には、MO（光磁気ディスク）100が装填、取出し自在に装填されるMO装填口51aが示されている。

【0038】また、このコンピュータシステム50は、内部構成上は、図4に示すように、各種のプログラムが実行されるCPU55、実行されるプログラムやデータの一時的な格納領域として使用されるメモリ56、キーボード53との間でデータの受け渡しを行なうキーボードインターフェース57、マウス54の操作に伴うデー

タを伝えるマウスインターフェース58、画像表示装置52に表示用のデータを伝える表示インターフェース59、図3に示すMO装填口51から装填されたMO100を駆動するMOドライブ60、および内蔵されたハードディスク62を駆動するハードディスクドライブ61が備えられており、それらは、図4に示すように、バス63で互いに接続されている。

【0039】ここでは、図3、図4に示すコンピュータシステム50内において、MO100に格納されたコンテンツの使用権をハードディスク62に委譲する場合を説明するが、使用権の単純な移動、あるいは、使用可能回数が設定されている場合において、その使用可能回数以内の一部の使用可能回数を初回に委譲する場合については、図1、図2を参照して既に説明済であるため、以下では、初回に委譲した使用可能回数を使い果たし、所定の使用可能回数を再度委譲する場合について説明する。また、図1、図2を参照した説明は、本発明の理解のために概念的な説明を行なったが、ここではより詳細な説明を行なう。

【0040】図5は、MO100に格納されたコンテンツの使用権をハードディスク62に委譲する手順を示す図である。この図5には、アプリケーション64とドライブ20が示されている。アプリケーション64は、CPU55で実行される、コンピュータシステム50の操作者により直接に操作が可能なプログラムであって、ここでは、MO100内のコンテンツの使用権をハードディスク62に委譲することを指示するプログラムをあらわしている。また、ドライブ20は、ここでは、図4に示すMOドライブ60とハードディスクドライブ61との複合体である。MO100に格納されたコンテンツの使用権をハードディスク62に委譲する手順を以下に説明するが、ここではMO100に、委譲しようとしているコンテンツを残り10回使用することができる使用権が残っており、そのうちの3回の使用権をハードディスク62に委譲するものとして説明する。

【0041】ここでは簡単のため、委譲され得るコンテンツは1つのみ存在するものとし、コンテンツと称するときは、その委譲される（あるいはその委譲によりハードウェア62に使用権が移った）コンテンツを意味するものとする。

(1) 先ず、アプリケーション64からドライブ20に向けて、コンテンツの委譲元がMO100であり、コンテンツの委譲先がハードディスク62であることを、ドライブ20に向けて指定する（図5（A））。

【0042】(2) するとドライブ20は、MO100およびハードディスク62をアクセスするための準備を行ない、ドライブ20は、それらの準備が整った段階で、アプリケーション64に対し準備が整ったことを報告する（図5（B））。

(3) すると、アプリケーション64では、ドライブ2

0がアプリケーションに送る情報を隠蔽するためのパスワードをドライブ20 (MOドライブ60とハードディスクドライブ61との双方) に送るとともに、MO100のセキュアエリア (図1, 図2参照) に格納されている使用権情報 (ここでは、上述の前提どおり、使用可能回数をあらわす情報を使用権情報としており、MO100には、現在10回使用可能であることをあらわす使用権情報‘10’が格納されているものとする) を読み出す命令をドライブ20に向けて発行する (図5 (C))。

【0043】 (4) すると、ドライブ20を構成するMOドライブ60 (図4参照) 内では、以下の処理が実行される。ここで、MOドライブ60内にもCPUが搭載されており、さらに、装填されたMO100をアクセスするためのマイクロプログラムが搭載されており、それらMOドライブ60のハードウェアとソフトウェアとを合わせたファームウェアがMOドライブ60における処理を実行することになる。

【0044】 (4-1) MO100のMIDエリア (図1, 図2のMIDエリア11参照) からMO100のメディアIDを読み出す。

(4-2) MO100のセキュアエリア (図1, 図2のセキュアエリア12参照) から、メディアIDで暗号化された使用権情報を読み出す。

(4-3) その読み出した使用権情報をメディアIDで復号化する。

【0045】 (4-4) 上述 (3) のステップにおいてアプリケーション64から送られてきたパスワードで、復号化された使用権情報をエンコードする。

(4-5) そのエンコードされた情報をアプリケーション64に伝える (図5 (D))。

(5) すると、アプリケーション64は、以下の処理を実行する。

【0046】 (5-1) MOドライブ60から送られてきた使用権情報をパスワードでデコードする。

(5-2) そのデコードされた使用権情報があらわす使用可能回数がこれ以上使用できないことをあらわす‘0’でないことを確認する (ここでは、説明の前提として使用可能回数10回をあらわす‘10’が設定されており、‘0’ではない)。

【0047】 (5-3) 今度は、ドライブ20に向けて、使用権の委譲先であるハードディスク62の、使用権情報を読み出す命令を発行する (図5 (E))。尚、前述したように、ここでは説明の前提として、ハードディスク62には、前回、コンテンツを何回か使用することのできる使用権が設定され、その使用可能回数が‘0’になった場合を想定している。

【0048】 (6) すると、ハードディスク62を駆動するハードディスクドライブ61では以下の処理が実行される。ハードディスクドライブ61にもCPUやマイ

クロプログラムが備えられており、ハードディスクドライブ61における処理も、MOドライブ60における処理と同様、それらハードウェアとソフトウェアとの複合体としてのファームウェアにより実行される。

【0049】 (6-1) ハードディスク62のMIDエリア (図1, 図2のMIDエリア31参照) からハードディスク62のメディアIDを読み出す。

(6-2) ハードディスク62のセキュアエリア (図1, 図2のセキュアエリア32参照) から、ハードディスク62のメディアIDで暗号化された使用権情報を読み出す。

【0050】 (6-3) その読み出した使用権情報を、ハードディスク62のメディアIDで復号化する。

(6-4) 上述の (3) のステップにおいてアプリケーション64から送られてきたパスワードで、その復号化された使用権情報をエンコードする。(6-5) そのエンコードされた使用権情報をアプリケーション64に伝える (図5 (F))。

【0051】 (7) すると、アプリケーション64は、以下の処理を実行する。

(7-1) ハードディスクドライブ61から送られてきた使用権情報をパスワードでデコードする。

(7-2) そのデコードされた使用権情報が使用可能回数‘0’をあらわしていることを確認する。

【0052】 もし使用可能回数が‘0’でなく、まだ使用可能であることをあらわしているときは、本実施形態では、まだ使用可能である旨表示画面52a (図3参照) に表示してオペレータにその旨通知し、この段階で処理を中断する。ここでは説明の前提として使用可能回数は‘0’であり、この場合、さらに以下の処理に進む。

【0053】 (7-3) ハードディスク62に新たに設定される使用可能回数 (ここでは説明の前提に基づいて3回) をあらわす情報 (新回数情報と称する) をパスワードでエンコードしてドライブ20 (MOドライブ60とハードディスクドライブ61との双方) に送る (図5 (G))。

(8) MOドライブ60では、この新回数情報を受けて以下の処理が実行される。

【0054】 (8-1) MO100のメディアIDを読み出す。

(8-2) MO100のセキュアエリアに格納されている、MO100のメディアIDで暗号化された状態の使用権情報を読み出す。

(8-3) その暗号化された使用権情報をMO100のメディアIDで復号化して使用可能回数‘10’を取り出す。

【0055】 (8-4) アプリケーション64から送られてきた、パスワードでエンコードされた新回数情報を、上述の (3) のステップで送られてきているパスワ

ードでデコードして使用可能回数‘3’を取り出す。

(8-5) MO100にそれまで格納されていた使用可能回数‘10’からハードディスク62に譲渡しようとしている使用可能回数‘3’を差し引いて新たな使用可能回数‘7’を得る。

(8-6) その新たな使用可能回数‘7’をあらわす新たな使用権情報をMO100のメディアIDで暗号化する。

【0056】(8-7) その暗号化された新たな使用権情報を、それまでMO100に格納されていた、使用可能回数‘10’をあらわす使用権情報に上書きする。これにより、MO100には使用可能回数‘7’が設定される。

(9) 一方、ハードディスクドライブ61では、上述の(7-3)のステップで送られてきた新回数情報を受けて、以下の処理が実行される。

【0057】(9-1) ハードディスク62のメディアIDを読み出す。

(9-2) アプリケーション64から送られてきた、パスワードでエンコードされた新回数情報を、上述の(3)のステップで送られてきているパスワードでデコードして使用可能回数‘3’を取り出す。

(9-3) そのデコードにより取り出された使用可能回数‘3’をあらわす新たな使用権情報をハードディスク62のメディアIDで暗号化する。

【0058】(9-4) その暗号化された新たな使用権情報を、ハードディスク62に格納されていた、使用可能回数‘0’をあらわす使用権情報に上書きする。これにより、ハードディスク62には、使用可能回数‘3’が設定される。

(10) 以上の使用権委譲の処理が完了したことが、ドライブ20からアプリケーション64に通知される。

【0059】以上のようにしてコンテンツの使用権の委譲(ここでは使用権の一部の委譲)が行なわれる。尚、図5を参照した以上の説明では、MO100からハードディスク62への、コンテンツ自体および暗号化されたコンテンツを復号化するための鍵の移動については言及されていないが、前述したように、ここでは、コンテンツの使用可能回数の再度の設定の場合を説明しており、したがってコンテンツ自体および、それを復号化するための鍵は初回の委譲時に既にハードディスク62に渡されていることを前提としている。コンテンツ自体は、MO100から初回の委譲時に暗号化された形式のままハードディスク62に移動(複製)されており、また上記の説明は、鍵はそれぞれのメディアIDで使用権情報とは独立に暗号化されてそれぞれのセキュアエリアに格納されていることを前提としている。

【0060】尚、図5を参照して説明した実施形態では、上述したように、アプリケーション64とドライブ20とが様々なコミュニケーションを行ないながらコン

テンツの使用権の委譲の処理を進めているが、このようなコンテンツ委譲処理に代え、アプリケーション64からは、使用権を委譲しようとしているコンテンツ、そのコンテンツの使用権の委譲元(ここではMO100)、委譲先(ここではハードディスク62)、および委譲しようとしている、使用権の回数を指定し、その後はドライブ20(ここではMOドライブ60とハードディスクドライブ61との双方)に処理を任せ、アプリケーション64とは独立にドライブ20において上記の委譲処理を実行し、委譲処理が終了した段階、および何らかの不都合により委譲処理が正常に行なわれなかった(例えばMO100に委譲を指定された使用可能回数未満の使用可能回数しか残っていなかった、あるいはハードディスク62に前回に委譲を受けた使用可能回数がまだ‘0’になっていなかった、など)ときのみ、アプリケーション64に報告するように構成してもよい。

【0061】また、上記の委譲処理60は、上記の説明ではMOドライブ60とハードディスクドライブ61とで分担して実行しているが、それらMOドライブとハードディスクドライブ61とのうちの一方はアクセス専用とし、上記の委譲処理は、専らもう一方の側で行なうように構成してもよい。図6は、本発明のライセンス委譲装置の一実施形態が組み込まれたコンピュータネットワークの一例を示す図、図7は、そのコンピュータネットワークを構成するあるコンピュータシステムから別のコンピュータシステムに対し、コンテンツの使用権を委譲する際の手順を示す図である。

【0062】ここには、コンテンツ管理用のコンピュータシステム70と、コンテンツを使用する側の2台のコンピュータシステム80、90が示されており、それら3台のコンピュータシステム70、80、90は、通信回線200を介して互いに接続されている。各コンピュータシステム70、80、90は、それぞれが図3に示すコンピュータシステム50と同様の構成を備えている。すなわち、各コンピュータシステム70、80、90は、各本体部71、81、91、各画像表示装置72、82、92、各キーボード73、83、93および各マウス74、84、94を備えており、さらに各コンピュータシステム70、80、90は、それぞれが図4に示す内部構成と同様の内部構成を備えている。詳細説明は省略する。

【0063】ここでは、コンテンツ管理用のコンピュータシステム70は、ある会社の本店に設置され、コンテンツを使用する側のコンピュータシステム80、90はその会社の各支店に設置されているものとする。以下では、説明の簡単のため、本店、および各支店に設置されたコンピュータシステム70、80、90を、そのまま本店70、支店80、支店90と称する。

【0064】ここでは本店で、各種のコンテンツの全支店分のライセンスを購入し、その本店から各支店にライ

センスを分配し、かつ、その本店で全支店分のライセンスを管理しているものとする。すなわち、ここでは、同一のコンテンツであっても本店において必要な数の使用権を購入し、そのコンテンツを必要とする支店にその使用権を分配する。ここでいう同一のコンテンツについての必要な数の使用権は、そのコンテンツの使用回数を意味するものではなく、同一の本を複数冊（例えば 3 冊）購入すると同様に同一のコンテンツの使用権を必要に応じた数だけ購入し、ここではその購入した数の使用権を意味している。本店では、各コンテンツについて、購入した使用権の数から支店に対し使用権を頒布した数の残りの数が管理されており、各支店では、同一のコンテンツについての複数の使用権は不要であって、各コンテンツについて自分の支店に使用権が存在するか否かのみを管理している。本店および各支店では多数のコンテンツの使用権情報が管理されており、ここではそれら多数のコンテンツの使用権情報の一覧を「許諾情報」と称する。

【0065】ここでは、本店 70 から各支店 80、90 に対し、既に様々なコンテンツの使用権が委譲されており、さらに今回、本店 70 からある支店（ここでは支店 80 とする）に対しあるコンテンツの使用権を委譲するものとし（ここでは、使用権の新たな委譲を行なおうとしているコンテンツを「新コンテンツ」と称する）、ここでは、その新コンテンツの使用権を支店 80 に委譲する場面について説明する。ここでは、新コンテンツの使用権は、本店 70 のハードディスクから支店 80 のハードディスクに委譲されるものとする。

【0066】（1）先ず本店 70 から支店 80 に向けて新コンテンツの使用権を委譲する旨連絡する（図 7（A））。

（2）すると支店 80 ではその連絡を受けて、支店 80 のハードディスクを準備状態にし、アクセスの準備が整うと本店 70 に対し準備ができたことを報告する（図 7（B））。

【0067】（3）すると本店 70 では、支店 80 から送られてくる情報を隠蔽するためのパスワードを支店 80 に送出し、さらに支店 80 のハードディスクのセキュアエリアに格納されている許諾情報（複数のコンテンツそれぞれの使用権の有無をあらわす情報の一覧）を送るよう命令を発行する（図 7（C））。

（4）支店 80 では、この命令を受けて以下の処理を実行する。

【0068】（4-1）支店 80 のハードディスクのメディア ID を読み出す。

（4-2）支店 80 のハードディスクのセキュアエリアから、そのハードディスクのメディア ID で暗号化された許諾情報を読み出す。

（4-3）その読み出した許諾情報を読み出したメディア ID で復号化する。

（4-4）上記の（3）のステップにおいて本店 70 から送られてきたパスワードで、その復号化された許諾情報と、さらに支店 80 のハードディスクのメディア ID をエンコードする。

【0069】（4-5）そのエンコードされた許諾情報およびメディア ID を本店 70 に送る（図 7（D））。

（5）すると、本店 70 では、以下の処理を実行する。

（5-1）支店 80 から送られてきた許諾情報およびメディア ID をパスワードでデコードする。

【0070】（5-2）そのデコードされた許諾情報を見て、これから支店 80 に使用権を移そうとしている新コンテンツに関する使用権が支店 80 に存在しないことを確認する。これは、同一の支店に対し同一のコンテンツの使用権を重複設定するのを避けるためである。

（5-3）本店 70 のハードディスクのメディア ID を読み出す。

【0071】（5-4）本店 70 のハードディスクのセキュアエリアから、そのハードディスクのメディア ID で暗号化された許諾情報、および、同じくそのメディア ID で暗号化された、使用権を許諾しようとしているコンテンツを復号化するための鍵を読み出す。

（5-5）その読み出した許諾情報および鍵を、読み出したメディア ID で復号化する。

【0072】（5-6）その復号化された許諾情報を参照して、支店 80 に使用権をあらたに委譲しようとしているコンテンツ（新コンテンツ）に関する使用権に残りがあることを確認する。残りがなくなるときは、その新コンテンツの使用を許諾することができない旨支店 80 に伝えることになるが、ここでは、その新コンテンツの使用権が本店 70 に残っているものとする。

【0073】（5-7）上記の（5-1）のステップでデコードした、支店 80 の許諾情報中の、新コンテンツの使用権をあらわす情報を「使用権なし」から「使用権有り」に書き換える。

（5-8）その書き換えた許諾情報、および鍵の双方をパスワードでエンコードする。

【0074】（5-9）本店 70 のハードディスクのユーザエリアから、暗号化された新コンテンツを読み出す。

（5-10）そのエンコードされた許諾情報および鍵、および暗号化されたままの新コンテンツを支店 80 に送る（図 7（E））。

（5-11）また、本店 70 内において、上記の（5-5）のステップで復号化した本店 70 の許諾情報中の、支店 80 に今回使用権を許諾した新コンテンツに関する使用権の数に関する情報を 1 だけ減算することにより新たな許諾情報に更新する。

【0075】（5-12）そのようにして更新された新たな許諾情報を、本店 70 のハードディスクのメディア ID で暗号化する。

(5-13) その暗号化された新たな許諾情報を、本店 70 のハードディスクのセキュアエリアに、そこにそれまで格納されていた更新前の許諾情報に代えて格納する。

【0076】(6) 支店 80 では、上記の(5-10)のステップで送られてきた、エンコードされた許諾情報および鍵、および暗号化された新コンテンツを受け取り、以下の処理を実行する。

(6-1) 受け取った新コンテンツを、暗号化されたまま自分(支店 80)のハードディスクのユーザエリアに、10 格納する。

【0077】(6-2) 受け取った許諾情報および鍵を、上述のステップ(3)で送られてきているパスワードでデコードする。

(6-3) 自分(支店 80)のハードディスクのメディア ID を読み出す。

(6-4) パスワードでデコードされた許諾情報および鍵を、その読み出したメディア ID で暗号化する。

【0078】(6-5) その暗号化された許諾情報および鍵を、自分(支店 80)のハードディスクのセキュア 20 エリアに、それまで格納されていた許諾情報を書き換えるようにして格納する。以上により、その新コンテンツの使用権が本店 70 から支店 80 に委譲される。

【0079】以上の各実施形態に示すように、本発明のライセンス委譲装置は、1 台のコンピュータ等からなる 1 台の装置内においても、あるいは複数台のコンピュータ等を接続したネットワーク内においても実現可能である。

【0080】

【発明の効果】以上説明したように、本発明によれば、30 コンテンツに関し権利を有する者の権利を犯すことなく、そのコンテンツを複製したり頒布したりすることができる。

【図面の簡単な説明】

【図 1】本発明のライセンス委譲装置の一実施形態を示す構成図である。

【図 2】図 1 に示すライセンス委譲装置の説明のための模式図である。

【図 3】本発明のライセンス委譲装置の一実施形態が搭載されたコンピュータシステムの一例を示す外観斜視図 40 である。

【図 4】図 3 に外観を示すコンピュータシステムの構成を示すブロック図である。

【図 5】MO に格納されたコンテンツの使用権をハード

ディスクに委譲する手順を示す図である。

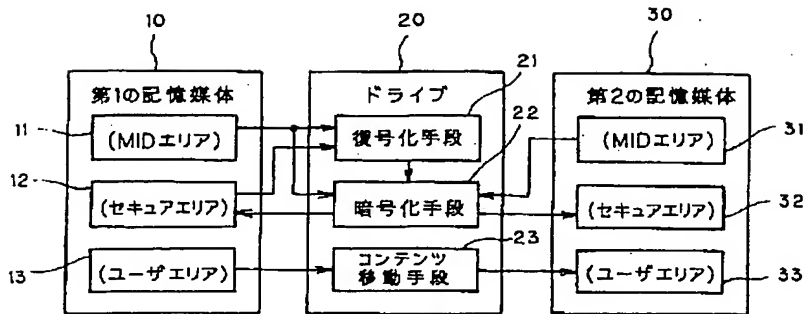
【図 6】本発明のライセンス委譲装置の一実施形態が組み込まれたコンピュータネットワークの一例を示す図である。

【図 7】図 6 に示すコンピュータネットワークを構成するコンピュータシステムから別のコンピュータシステムに対し、コンテンツの使用権を委譲する際の手順を示す図である。

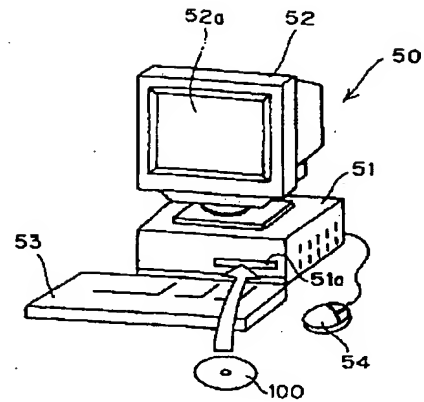
【符号の説明】

10	第 1 の記憶媒体
11	MID エリア
12	セキュアエリア
13	ユーザエリア
20	ドライブ
21	復号化手段
22	暗号化手段
23	コンテンツ移動手段
30	第 2 の記憶媒体
31	MID エリア
32	セキュアエリア
33	ユーザエリア
41, 42	使用権情報
50	コンピュータシステム
51	本体部
51a	MO 装填口
52	画像表示装置
52a	表示画面
53	キーボード
54	マウス
55	CPU
56	メモリ
57	キーボードインターフェース
58	マウスインターフェース
59	表示インターフェース
60	MO ドライブ
61	ハードディスクドライブ
62	ハードディスク
70, 80, 90	コンピュータシステム
71, 81, 91	本体部
72, 82, 92	画像表示装置
73, 83, 93	キーボード
74, 84, 94	マウス
100	MO (光磁気ディスク)
200	通信回線

【図 1】

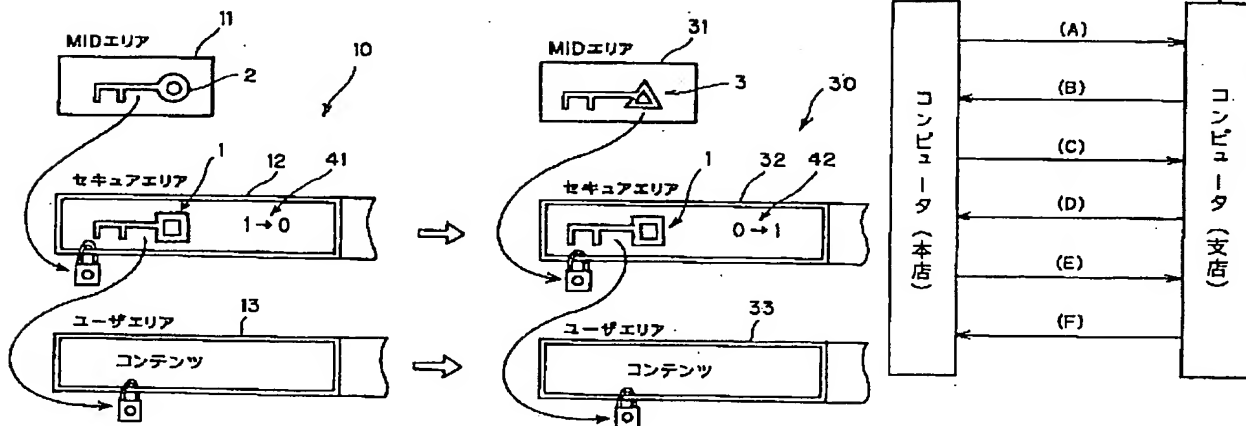


【図 3】

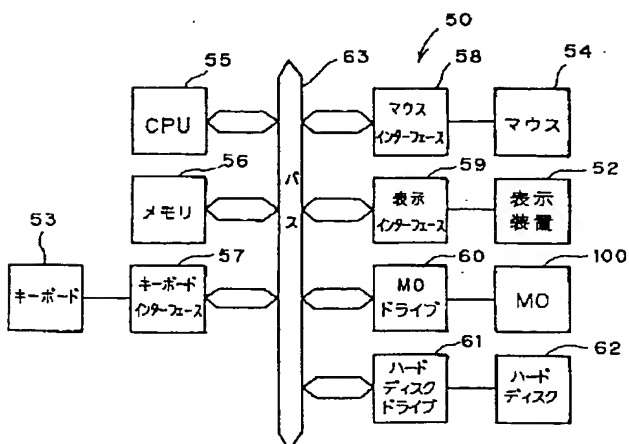


【図 7】

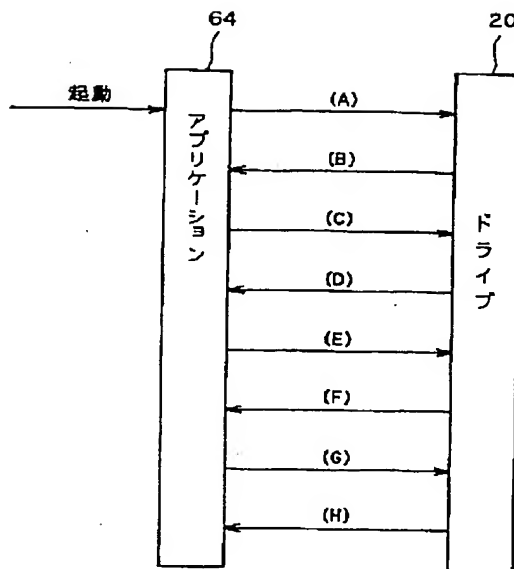
【図 2】



【図 4】



【図5】



【図6】

